REMARKS

In response to the Office Action dated February 15, 2005, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

In response to the objection to the specification, the typographical error identified in the Office Action has been corrected.

Claim 1 was rejected under the second paragraph of 35 U.S.C. §112, on the grounds that the term "some" was considered to be indefinite. In response thereto, claim 1 has been amended to remove this term.

All pending claims were rejected under 35 U.S.C. §103, on the grounds that they were considered to be unpatentable over the Leppek patent (U.S. 5,933,501) in view of the Kocher et al patent (U.S. 6,278,783). For the reasons presented below, it is respectfully submitted that these patents do not disclose all of the features recited in the claims. Consequently, any logical combination of their teachings would not result in the claimed subject matter.

Claim 1 recites a countermeasure method that includes the step of executing a first set of instructions in a cryptographic algorithm with a first manipulating means to deliver output data on the basis of input data. Referring to the exemplary embodiment of Figure 7, the SBOX operation is executed in computation round T2 with a first manipulating means that is implemented with the constants table TC_0.

Claim 1 goes on to recite the step of executing another set of instructions with "other manipulating means that are derived from said first manipulating means...." Referring again to Figure 7, during computation round T1, the SBOX operation is carried out with the constants table TC_1. As illustrated in Figures 6 and 9 of the

application, the constants table TC_1 is derived from the constants table TC_0 in that the output data of the table TC_1 is the complement of that delivered by the table TC_0.

The rejection of claim 1 states that the Leppek patent discloses the features of claim 1 that are discussed above, with specific reference to Figure 2 and column 4, lines 7-51. The Leppek patent discloses a compound encryption scheme in which a plurality of different types of encryption routines are successively applied to data that is to be encrypted. As disclosed in the patent, each individual encryption routine can be a conventional encryption operator, "such as, PGP, DES, etc. routines." (Column 4, lines 14-17). It appears that the Office Action is interpreting two successive encryption routines as corresponding to the first manipulating means and other manipulating means that are recited in the claim. However, the patent does not disclose that one of these encryption routines is "derived from [the other] manipulating means. . . ," as recited in claim 1 and alleged in the Office Action. Rather, the patent discloses that the various encryption routines can be entirely different types of encryption operators, such as PGP and DES. These two types of encryption algorithms are not related, in the sense that one is derived from the other. Rather, they are entirely independent techniques for encrypting data.

Accordingly, it is respectfully submitted that the Leppek patent does not disclose all of the features that are alleged in the Office Action.

In addition to the features discussed above, claim 1 further recites that the second, or "other," manipulating means is derived from the first manipulating means "by complementation of at least one of said input data and said output data." The Office Action acknowledges that the Leppek patent does not disclose this concept,

and therefore relies upon the teachings of the Kocher patent, particularly at column 6, lines 29-63, and column 9, lines 5-23.

The Kocher patent, like the present invention, is concerned with an attacker's ability to derive secure information by observing a series of operations performed in a cryptographic system. However, the approach that is employed by the Kocher patent is substantially different from the present invention. Specifically, the Kocher patent discloses a technique wherein the message to be encrypted, and/or the encryption keys, are disguised, or "blinded," prior to processing by the DES algorithm. The blinding is accomplished by generating two values which, when combined with one another by means of an Exclusive-Or operation, result in the original message. Permutations of these values are employed to perform the encryption.

It is respectfully submitted that the Kocher patent does not contain any teachings that would lead a person of ordinary skill in the art to the claimed invention, even when applied to the disclosure of the Leppek patent. As noted in the Office Action, the Kocher patent discloses a modification of the DES algorithm. A logical application of these teachings to the Leppek patent, therefore, would be to modify the particular encryption routine that is based upon the DES algorithm. In other words, when using that routine, the message and/or encryption keys can be blinded, as taught by the Kocher patent. This result is not the same as the presently claimed invention. In particular, there is no suggestion in these combined teachings that a second manipulating means, e.g. one of the encryption routines 110-i of the Leppek patent, is derived from another one of the encryption routines through the complementation of at least one of the input data or output data of that other routine.

At best, the Kocher patent only suggests that an individual one of the encryption routines, namely one that is based upon the DES algorithm, can be modified to reduce the likelihood of information leakage. Neither the Leppek patent nor the Kocher patent discloses that successive encryption routines performed on data have any relationship to one another, much less one in which the input or output data of one is the complement of that of the other.

Accordingly, it is respectfully submitted that the subject matter of claim 1 is not suggested by the Leppek and Kocher patents, whether considered individually or in combination. Additional differences between the present invention and the teachings of those references are set forth in dependent claims 2-10. In light of the distinctions identified above, a detailed discussion of these other differences is submitted to be unnecessary at this time.

For analogous reasons, it is respectfully submitted that the subject matter of claims 13-16 is likewise not suggested by the references. Claim 13 recites an electronic component that comprises a program memory having a plurality of different manipulating means stored therein, and a processor which executes instructions in a cryptographic algorithm, in accordance with a selected one of the manipulating means. The claim further recites a means for generating a random value for selecting the manipulating means to be employed during a given execution of the algorithm.

It is respectfully submitted that this claimed subject matter is not taught by the Leppek patent, whether or not it is considered in view of the Kocher patent. Even if the different encryption routines of the Leppek patent are interpreted to be different manipulating means, there is no suggestion that the particular manipulating means

that is selected for a given execution of the algorithm is based upon a random value. Rather, the Leppek patent specifically discloses that the sequence of encryption routines is based upon a predetermined sequence, and that any two successive routines must be different from one another (see column 4, lines 49-51).

The Office Action refers to the simplest form of the encryption technique disclosed in the Leppek patent, where two different encryption routines are utilized. If random selection were used, the probability that two successive routines would be the same is as high as the probability that they would be different. Such a result is clearly contrary to the teachings of the Leppek patent. In other words, the Leppek patent teaches away from using random selection of the encryption operators. The Kocher patent does not contain any disclosure that would overcome this difference.

For at least these reasons, therefore, it is respectfully submitted that the subject matter of claim 13, and its dependent claims, are not suggested by the Leppek and Kocher patents, whether considered individually or in combination.

In view of the foregoing, it is respectfully submitted that all pending claims are patentable over the prior art of record. Reconsideration and withdrawal of the rejections are respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: May 12, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620